FILED
2025 Jun-06 PM 04:08
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

PAUL WIEZOREK, individually and on behalf of all others similarly situated,	)	**CASE NO.: _____**
Plaintiff,	)	**JURY TRIAL DEMANDED**
v.	)	
BRADFORD HEALTH SERVICES, LLC,	)	**CLASS ACTION**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Paul Wiezorek ("Mr. Wiezorek" or "Plaintiff"), on behalf of himself and all others similarly situated, file this Class Action Complaint against Bradford Health Services, LLC, ("Defendant") and allege as follows:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII"), protected health information ("PHI"), as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), other medical and financial information, (collectively, "PII/PHI"), and for failing to provide timely, accurate, and adequate notice to Plaintiff and other individuals who are Class Members (defined below) that the integrity of their PII/PHI had been compromised and stolen.

2. Defendant is a collection of "top-quality addiction treatment programs throughout the Southeast that are in-network with most major insurance providers and recognized by leading

carriers for our outcomes and complete continuum of care."[1]

3. Defendant has been "successfully treating alcohol and drug addiction since 1977."[2]

4. On or about December 8, 2023, Defendant noticed unusual activity within its network systems. After noticing this activity, Defendant immediately took steps to secure their network systems and brought in independent digital forensics and incident response firm to investigate the suspicious activity.[3]

5. Defendant learned that an unknown actor gained unauthorized access to Defendant's network system and acquired certain files containing PII/PHI of Plaintiff and Class Members such as individuals' names, driver's license numbers, dates of birth, medical information (including diagnosis and treatment information, physician names, and Medical Record numbers), health insurance information, financial account numbers, passport numbers, payment card numbers plus a means of access to the account, and/or Social Security numbers."[4]

6. On or around May 30, 2025, Plaintiff and Class Members received notice letters from Defendant informing Plaintiff and Class Members of the Data Breach.[5]

7. Ther Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Patients' PII/PHI.

8. Defendant disregarded the rights of Plaintiff and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its

---

[1] *See* http://bradfordhealth.com/about/ (last visited June 5, 2025).
[2] *Id*.
[3] *See Bradford Health Services Notice of Data Security Incident sent to Plaintiff* (**Exhibit A**).
[4] *See Notice of Data Security Incident* posted on Defendant's website http://bradfordhealth.com/notice-of-data-security-incident/
[5] *See* **Exhibit A**.

data networks, systems and/or servers were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Patients' PII/PHI; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach; and failing to provide comprehensive and effective credit protection services after notification of the Data Breach.

9. As a result of Defendant's failure to implement and follow basic security procedures, Defendant's Patients' PII/PHI is now in the hands of thieves who, upon information and belief, have committed criminal acts against the Patients by misusing their data and/or have published and/or sold their data on the internet (i.e., the "dark web") for others to view, access, and/or misuse. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and financial fraud.

10. Plaintiff, on behalf of all others similarly situated, allege claims for negligence, wantonness, negligence *per se*, breach of express and/or implied contracts, and unjust enrichment and seek to compel Defendant to fully and accurately disclose the nature of the Data Breach and the information that has been compromised, in addition to adopting sufficient security practices and protocols to safeguard the Patients' PII/PHI that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future, because the risk of future harm from another data breach from Defendant is both imminent and substantial.

11. Defendant flagrantly disregarded Plaintiff's and the other Class Members' privacy rights by intentionally, willfully, recklessly, negligently and/or wantonly failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized

disclosure.

12. Plaintiff's and Class Members' PII/PHI was improperly handled and stored and was otherwise not kept in accordance with federally prescribed, industry standard security practices and procedures. As a result, Plaintiff's and Class Members' PII/PHI was compromised, accessed, and stolen.

13. Defendant's intentional, willful, reckless, negligent and/or wanton disregard of Plaintiff's and Class Members' rights directly and/or proximately caused a substantial unauthorized disclosure of Plaintiff's and Class Members' PII/PHI. The improper use of PII/PHI by unauthorized third parties resulted in an adverse impact on the credit rating and finances of Plaintiff and the Class Members.

14. The type of wrongful PII/PHI disclosure made by Defendant is the most harmful because it generally takes a significant amount of time for a data breach victim to become aware of misuse of that PII/PHI. Additionally, it takes a significant amount of time to protect oneself against attempted and actual identity theft and financial fraud.

15. On behalf of himself and Class Members, Plaintiff bring this lawsuit because he has suffered, and will continue to suffer, actual injuries and damages as a direct and/or proximate result of Defendant's wrongful actions and/or inactions and the resulting Data Breach including, but not limited to, unauthorized disclosure, publication, and dissemination of their PII/PHI on the internet, misuse of their PII/PHI, identity theft, financial fraud, loss of money and time in combatting the attempted and actual identity theft and fraud, and emotional distress.

16. Additionally, Plaintiff seeks injunctive relief as a direct and/or proximate result of Defendant's wrongful actions and/or inactions to prevent Defendant's next data breach, which is both likely and imminent.

17. Defendant's wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiff and Class Members at an imminent, immediate, substantial, and continuing increased risk of identity theft and identity fraud.[6] Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, released a 2012 Identity Fraud Report (the "Javelin Report") quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII/PHI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity theft and/or identity fraud has not yet been discovered or reported and a high probability that criminals who now possess Plaintiff's and Class Members' PII/PHI—if they have not already misused the data—will do so later or re-sell it. Even if they are without such loss now, Plaintiff and Class Members are entitled to relief and recovery because Plaintiff and Class Members are under an imminent risk that their information will soon be misused similar to the misuse other Plaintiff have already experienced.

18. Defendant's wrongful actions and/or inactions constitute common law negligence and common law invasion of privacy by public disclosure of private facts. Further, Defendant's wrongful actions and/or inactions constitute a breach of contract, breach of fiduciary duty, breach of confidence, and unjust enrichment.

19. Plaintiff, on behalf of himself and the Class Members, seek actual damages, economic damages, nominal damages, exemplary damages, injunctive relief, and costs of suit.

[6] According to the United States Government Accounting Office, the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities, such as when PII/PHI is used to commit fraud or other crimes (credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services)).

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and Plaintiff, as well as numerous Class members, are citizens of states other than Defendant's states of citizenship. Upon information and belief, at least one of Defendant's LLC members is a citizen of Alabama.

23. This Court has personal jurisdiction over the parties in this case. Defendant conducts business in this District, has its principal place of business located in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

24. Venue is proper in this District pursuant to 28 U.S.C. §1391(b) because, at all relevant times, Defendant's principal place of business is in this District and Defendant routinely conducts business throughout the District.

PARTIES

Plaintiff Paul Wiezorek

25. Mr. Wiezorek is an adult resident and citizen of North Platte, Nebraska. He is a former patient of Defendant and received services in 2020. Mr. Wiezorek suffered, and will continue to suffer, injuries and damages as set forth below.

26. As a condition to receive Defendant's services, Defendant required Mr. Wiezorek to provide and entrust it with his PII/PHI, including his health insurance information. Mr. Wiezorek would not have provided Defendant with his PII/PHI had he known that Defendant would not protect it as promised.

27. Upon information and belief, Mr. Wiezorek provided Defendant with PII/PHI including, but not limited to, his full name, mailing address, email address, telephone number, date

of birth, Social Security number, Driver's License number, medical and treatment information, billing and claims information, health insurance information, financial account information, and/or credit and debit card information.

28. On or about May 30, 2025, Mr. Wiezorek received notice from Defendant that his PII/PHI was compromised by the Data Breach.

29. Mr. Wiezorek's PII/PHI, which he entrusted to Defendant and which Defendant failed to properly safeguard, was viewed, accessed, and stolen from Defendant by unauthorized third parties, which directly and/or proximately caused him to suffer, and will continue to suffer, an injury-in-fact and actual damages.

Defendant Bradford Health Services, LLC

30. Defendant Bradford Health Services, LLC, does business in Alabama and across the South as addiction treatment and drug alcohol rehab facilities.[7] Defendant is an addiction recovery domestic limited liability company registered and qualified to do business in Alabama.

31. Defendant's principal place of business is in Jefferson County, Alabama located at 2101 Magnolia Avenue South, Suite 518 Birmingham, Alabama 35205. Additionally, Defendant is registered and qualified to do business in Alabama, and was doing business in Jefferson County, Alabama at all times materially relevant hereto.

32. Upon information and belief, at least one of Defendant's LLC members are citizens of Alabama.

33. Defendant has over 28 locations across the Southeast offering addiction treatment services.[8]

[7] *See* http://bradfordhealth.com/about/
[8] *See* http://bradfordhealth.com/bradford-locations/

34. Whenever reference in this Complaint is made to any act or transaction of Defendant, such allocations shall be deemed to mean that the principals, officers, employees, agents, and/or representatives of Defendant committed, knew of, performed, authorized, ratified and/or directed such transaction on behalf of Defendant while actively engaged in the scope of their duties.

BACKGROUND FACTS

A. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII/PHI*

35. In the regular course of its business, Defendant acquires, collects, stores and maintains possession, custody, and control of a wide variety and massive amount of information of Plaintiff's and Class Members' personal and confidential information, including: full names, addresses, telephone numbers, email addresses, dates of birth, Social Security numbers, Passport and Driver's License numbers, medical and treatment information, billing and claims information, health insurance information, financial account information, and/or credit and debit card information.

36. As a condition of engaging in health services, Defendant requires that its customers (patients) provide and entrust it with highly sensitive and confidential personal information.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendant assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII/PHI from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI. Plaintiff and Class Members, as current and former patients, relied

on Defendant to keep their PII/PHI confidential and securely maintained, to use their information for business purposes only, and to make only authorized disclosures of their sensitive information.

39. Defendant acknowledged its obligation to maintain the privacy of Patient PII/PHI entrusted to it by Plaintiff and Class Members through its Notice of Privacy Practices. Defendant's Notice of Privacy Practices represents, inter alia, that it is "required by law to maintain the privacy of your protected health information[.]"[9]

40. Defendant stored Plaintiff's and Class Members' PII/PHI, at a minimum, in an unprotected, unguarded, unsecured, and/or otherwise unreasonable location.

41. Defendant stored the Plaintiff's and Class Members' PII/PHI in a location that had inadequate security to prevent unauthorized access.

B. *Defendant's Data Breach*

42. Beginning as early as December 8, 2023, an unauthorized third party accessed Defendant's network and removed digital files containing Plaintiff's and Class Members' unencrypted PII/PHI.

43. On or about May 30, 2025, Plaintiff received a Notice Letter from Defendant informing Plaintiff of the Data Breach.[10]

44. Defendant's Notice of Data Security Incident sent to Plaintiff states, in relevant part:

> **What Happened.** On December 8, 2023, Bradford Health detected unusual activity within its network. Upon discovery, we immediately took steps to secure our network and engaged a leading, independent digital forensics and incident response firm to investigate. Based on that investigation, Bradford Health learned that an unknown actor gained unauthorized access to our network and acquired certain files, some of which contained individuals' personal and /or protected health information. With the assistance of a third-party data review team, we conducted a comprehensive review of all potentially impacted data to

[9] *See* http://bradfordhealth.com/notice-of-privacy-practices/
[10] *See* **Exhibit A**.

identify the individuals and information involved. On May 15, 2025, we determined that your information was impacted.

What Information Was Involved. The information that was potentially impacted during this incident may have included your name, as well as your date of birth, physician name, health care dates of service, treatment information or diagnosis treatment or procedure information, Medical Record Number (MRN), Patient Account Number (PAN), full face photograph or complete photograph.

What Are We Doing. As soon as Bradford Health discovered the incident, we took the steps described above and implemented measures to enhance the security of our network and reduce the risk of a similar incident occurring in the future. Bradford also reported the incident to law enforcement and is cooperating with any resulting investigation.[11]

45. Given the period of time during which unauthorized third parties had access to its files and the eighteen months between Defendant's discovery of the Data Breach and Defendant's public disclosure of it, the Plaintiff's and Class Members' PII/PHI has likely been bought and sold several times on the robust international cyber black market while Defendant denied the Plaintiff and Class Members any opportunity to take measures to protect their PII/PHI and privacy , which created an imminent and substantial risk of harm and identity theft that is ongoing.

46. Defendant's wrongful actions and/or inactions—to wit, failing to protect Plaintiff's and Class Members' PII/PHI with which it was entrusted—directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII/PHI without their knowledge, authorization, and/or consent. As a further direct and/or proximate result of Defendant's wrongful actions and/or inactions, Plaintiff and Class Members have suffered, and will continue to suffer, injuries and damages including, without limitation: (i) an increased and imminent risk of substantial harm; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) improper disclosure, dissemination and publication of their PII/PHI; (iv) criminal misuse of their PII/PHI; (v) identity theft; (vi) financial fraud; (vii) loss of privacy; (viii)

[11] *Id*.

out-of-pocket expenses incurred to mitigate the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ix) economic losses relating to the theft of their PII/PHI; (x) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (xi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xii) stress, anxiety and emotional distress.

47. As a result of Defendant's failure to properly safeguard and protect Plaintiff's and Class Members' PII/PHI, Plaintiff and Class Members' privacy has been invaded and their rights violated. Their compromised PII/PHI was private, confidential, and sensitive in nature and was left inadequately protected by Defendant.

48. Defendant's wrongful actions and/or inactions and the resulting Data Breach have caused Plaintiff and Class Members to suffer from identity theft and fraud, as well as placing them at a continuing increased, imminent and substantial risk of identity theft and identity fraud that is fairly traceable to the Data Breach.

C. *The Value of Personally Identifiable Information*

49. Identity theft occurs when a person's PII/PHI, such as the person's name, address, date of birth, Social Security number, billing and mailing addresses, phone number, email, credit card information, and health information is used without his or her permission to commit fraud or other crimes.[12]

50. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and

[12] *See* http://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited June 5, 2025).

that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[13] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [PII]."[14]

51. The FTC estimates that the identities of as many as nine million Americans are stolen each year.[15]

52. As a direct and/or proximate result of the Data Breach, Plaintiff and Class Members have been, and will continue to be, required to spend money and to take the time and effort to combat actual or suspected identity theft and fraud and also mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, placing "freezes" and "alerts" with the credit reporting agencies, reviewing, closing or modifying financial accounts, scrutinizing their credit reports and bank and credit accounts, and purchasing products to monitor their credit reports and financial accounts for unauthorized activity. Because Plaintiff's and Class Members' PII/PHI were stolen and/or compromised, they also now face a significantly heightened and imminent risk of harm and identity theft.

53. According to the FTC, identity theft is serious. "[Identity thieves] might steal your name and address, credit card, or bank account numbers, Social Security number, or medical insurance account numbers. And they could use them to buy things with your credit cards, get new credit cards in your name, open a phone, electricity, or gas account in your name, steal your tax

[13] Protecting Consumer Privacy in an Era of Rapid Change FTC Report (March 2012) (http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf) (last visited June 5, 2025).
[14] *Id*., at 11–12.
[15] *Id.*

refund, use your health insurance to get medical care, [or] pretend to be you if they are arrested."[16]

54. Theft of medical information, such as that included in the Data Breach here, is equally serious: "Medical identity theft is when someone uses your personal information—like your name, Social Security number, health insurance account number or Medicare number—to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care. If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[17]

55. Identity thieves also use Social Security numbers to commit other types of fraud. The GAO found that identity thieves use PII/PHI to open financial accounts and payment card accounts and incur charges in a victim's name. Ther type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, while in the meantime causing significant harm to the victim's credit rating and finances, which places Plaintiff and Class Members' at an increased and imminent risk of further future harm. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change, and their misuse can continue for years into the future.

56. Identity thieves use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves obtain jobs using stolen Social Security numbers, rent houses and

[16] *See* http://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last visited June 5, 2025).
[17] *See* http://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited June 5, 2025).

apartments, and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

57. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently, as well as show that he has done all he can to fix the problems resulting from the misuse.[18] Thus, a person whose PII/PHI has been stolen cannot obtain a new Social Security number until the damage has already been done.

58. Obtaining a new Social Security number, however, is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

59. Phone numbers are de facto identity documents, given the increasing reliance on using phone numbers as verification (i.e., two-factor authentication to access basic web pages.). A loss of a person's phone number can be as much of, if not more of, a risk than loss of a social security number—resulting in increased scam calls or loss of ability to access a web page.

[18] *See* http://consumer.ftc.gov/articles/do-you-need-new-social-security-number (last visited June 5, 2025).

60. As a direct and/or proximate result of Defendant's wrongful actions and/or inactions and the Data Breach, the thieves and/or their customers now have Plaintiff's and Class Members' PII/PHI. As such, Plaintiff and Class Members have not only already lost actual value but have been deprived, and will continue to be deprived, of the value of their PII/PHI.[19]

61. Plaintiff's and Class Members' PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for a number of years.[20] Identity thieves and other cyber criminals openly post stolen Social Security numbers, and other personal financial information on various Internet websites, thereby making the information publicly available.

62. The Data Breach was a direct and/or proximate result of Defendant's failure to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiff's and Class Members' PII/PHI from unauthorized access, use, and/or disclosure, as required by various federal and state regulations and industry practices.

63. Defendant flagrantly disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by not obtaining Plaintiff's and Class Members' prior written consent to disclose their PII/PHI to any other person—as required by HIPAA and other pertinent laws, regulations, industry standards and/or internal company policies.

---

[19] *See, e.g.,* John T. Soma, J. Zachary Courson, John Cadkin, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted); ABC News Report, http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2#.UGRgtq7yBR4 (last visited June 5, 2025).

[20] Companies, in fact, also recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. *See* T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

64. Defendant flagrantly disregarded and/or violated Plaintiff's and Class Members' privacy rights, and have harmed them in the process, by failing to establish and/or implement appropriate administrative, technical, and other safeguards required by industry standards to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI to protect against anticipated threats to the security or integrity of such information. Defendant's security deficiencies allowed unauthorized individuals to access, remove from its servers and networks, disclose, and/or compromise the PII/PHI of its Patients—including Plaintiff and Class Members.

65. Defendant's wrongful actions and/or inactions directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII/PHI without their knowledge, authorization, and consent. As a direct and proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and Class Members have incurred injuries and damages in the form of, *inter alia*: (i) an increased and imminent risk of future harm; (ii) the untimely and/or inadequate notification of the Data Breach; (iii) improper disclosure, dissemination and publication of their PII/PHI; (iv) criminal misuse of their PII/PHI; (v) identity theft; (vi) financial fraud; (vii) loss of privacy; (viii) out-of-pocket expenses incurred to mitigate the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) economic losses relating to the theft of their PII/PHI; (x) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (xi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (xii) stress, anxiety and emotional distress. Plaintiff's and Class Members' damages were foreseeable by Defendant.

D. ***Healthcare Organizations are Known High Risk Targets of Cyber Attackers***

66. The risk of harm to Plaintiff and Class Members from Defendant's failure to take precautionary measures was readily and clearly foreseeable. Not only was Defendant aware of the risks created by its inaction, but it was also in a unique position to know of the risk and prevent it.

67. Hospitals and healthcare organizations have become an attractive target of cyberattacks because they house a gold mine of sensitive, personally identifiable information for thousands of patients at any given time. From Social Security numbers and insurance policies to credit cards and emergency contacts' information, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[21] As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to quickly regain access to their data."[22]

68. Healthcare records are also preferred targets of cyberattacks because those records include far more information than other targets of cyberattacks (such as bank account numbers), and it has been estimated that medical records are **fifty times more valuable** on the black market than credit cards.[23]

69. As such, it has been reported that "[s]tolen healthcare records are the source of 95% of all identity theft[.]"[24] According to the 2019 Health Information Management Systems

---

[21] http://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited June 5, 2025).
[22] http://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targetedransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited June 5, 2025).
[23] *See* http://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/ (last visited June 5, 2025).
[24] *See* http://www.globenewswire.com/en/news-release/2022/03/31/2413675/0/en/Largest-

Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernible across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging emails to compromise the integrity of their targets."[25]

70. Despite years of rising awareness of healthcare organizations' position as the preeminent target of cyberattacks, the healthcare industry continues to suffer more data breaches than any other industry. According to Identity Theft Resource Center ("ITRC"), the healthcare industry in 2022, for the third year in a row, led all other industries in the number of data breaches.[26] Additionally, "[h]ealthcare organizations represented 19 percent of the 1,802 breaches reported in the 2022 IRTC report."[27]

71. Indeed, cyberattacks against healthcare organizations have become so prevalent that the Federal Bureau of Investigation ("FBI") has specifically warned that industry of the threat it faces and has given it recommendations to protect against data breaches.[28]

72. Therefore, the prevalence of such attacks, and the attendant, increased, and imminent risk of future attacks, was widely known to the public and anyone in the healthcare industry, including Defendant.

Healthcare-Data-Breaches-Reported-in-February-2022-Confirms-Need-for-Network-Security-Based-on-Zero-Trust-Microsegmentation.html (last visited June 5, 2025).

[25] *See* http://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited June 5, 2025).

[26] *See* http://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final.pdf (last visited June 5, 2025).

[27] http://www.prnewswire.com/news-releases/healthcare-remains-top-target-in-2022-itrc-breach-report-301730483.html (last visited June 5, 2025).

[28] *See* http://www.aha.org/cybersecurity-government-intelligence-reports/2022-09-12-fbi-pin-tlp-white-unpatched-and-outdated (last visited June 5, 2025).

E. Defendant*'s Conduct Violated HIPAA and Industry Standard Practices*

73. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII/PHI like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

74. Defendant's Data Breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of Patients', including Plaintiff's and Class Members', digital information;

d. Failing to properly encrypt Plaintiff's and Class Members' PII/PHI;

e. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

h. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

i. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

j. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94);

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*;

m. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

75. Defendant is still in possession of Plaintiff's and Class Members' PII/PHI and, without the injunctive relief requested herein, Plaintiff and Class Members remain at substantial risk of having their PII/PHI stolen again in a future data breach due to Defendant's woefully inadequate data security and cybersecurity. Defendant has not invested the necessary resources into data security or cybersecurity, and another future data breach is imminent and likely to occur at any time.

76. The substantial risk of harm to Plaintiff would be greatly reduced or eliminated by the injunctive relief requested herein, because the additional cybersecurity measures and policies would be capable of deterring would-be hackers and other cybersecurity threats—unlike Defendant current data security and cybersecurity measures, which have proven to be vulnerable to criminals.

77. Defendant violated federal and state statutes and industry standards to better secure its information privacy practices following the breach, which further created an imminent and substantial risk of future harm and identity theft.

78. Defendant also violated industry standards by shifting liability from its business practices to patients to mitigate the damages caused by the Data Breach. Patients cannot be expected to understand how to best mitigate damages from Defendant's enterprise-wide cybersecurity breaches.

PLAINTIFF'S FACTS

Plaintiff Paul Wiezorek

79. Mr. Wiezorek is a current patient of Defendant, in which he began receiving services from Defendant in 2020. Mr. Wiezorek has received services from Defendant again in 2021 and this year.

80. Defendant's conduct, which allowed the Data Breach to occur, caused, and will continue to cause, Mr. Wiezorek significant, actual injuries and harm, including but not limited to, the following—Mr. Wiezorek immediately devoted (and must continue to devote) time, energy, and money to: closely monitor his medical statements, bills, records, and credit and financial accounts; potentially change login and password information on any sensitive account even more frequently than he already does; more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack; search for suitable identity theft protection and credit monitoring services and pay for such services to protect himself; and place fraud alerts and/or credit freezes on his credit file. Mr. Wiezorek has taken, and will continue to take, to take these measures in order to mitigate his potential damages as a result of the Data Breach, since he continues to be at an increased, imminent risk of another future attack and harm.

81. Mr. Wiezorek has had to cancel one of his credit cards for fraudulent activity which he believes is related to the Defendant's Data Breach.

82. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse that is imminent and substantial. For this reason, Mr. Wiezorek – and all Class Members' – will need to maintain these heightened measures for years, and possibly his entire life.

83. Mr. Wiezorek greatly values his privacy, especially while receiving medical services. Mr. Wiezorek would not have obtained medical services from Defendant, or paid the amount he did to receive such, had he known that Defendant would negligently fail to adequately protect his PII/PHI.

84. Mr. Wiezorek – and all Class Members' – is also at a continued risk of imminent

harm because his PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased, imminent, and substantial risk of a future attack.

85. As a result of the Data Breach, and in addition to the time Mr. Wiezorek has spent and anticipates spending to mitigate the impact of the Data Breach on his life, Mr. Wiezorek also suffered emotional distress from the public release of his PII and PHI, which he believed would be protected from unauthorized access and disclosure. The emotional distress he experienced includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing his PII and PHI for the purposes of identity theft and fraud.

86. Additionally, Mr. Wiezorek has suffered, and will continue to suffer, damage to and diminution in the value of his highly sensitive and confidential PII/PHI—a form of property that Mr. Wiezorek entrusted to Defendant, and which was compromised as a result of the Data Breach Defendant failed to prevent. Mr. Wiezorek has also suffered a violation of his privacy rights as a result of Defendant's unauthorized disclosure of his PHI/PII.

87. Subsequent to the Data Breach, and in addition to the injuries alleged above, Mr. Wiezorek also experienced a significant increase in spam calls, emails, and texts that are fairly traceable to the Data Breach.

88. Mr. Wiezorek deals with the fallout of this Data Breach every day. He has spent multiple hours addressing the spam calls and texts which were a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Mr. Wiezorek otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Mr. Wiezorek lost was spent at Defendant's direction.

89. Mr. Wiezorek will continue taking additional time-consuming, necessary steps to

help mitigate the harm caused by the Data Breach, including continually reviewing Mr. Wiezorek's accounts for any unauthorized activity and screening spam calls and texts.

CLASS ACTION ALLEGATIONS

90. Plaintiff brings this class action, individually and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure:

> **All persons in the United States, excluding those persons residing in the state of Alabama, whose personal identifying information (PII) and personal health information (PHI) was exposed to unauthorized third parties as a result of the Data Breach discovered by BHS on or about December 8, 2023. (the "Nationwide Class").**

91. Excluded from the Class are the (i) owners, officers, directors, agents and/or representatives of Defendant and its parent entities, subsidiaries, affiliates, successors, and/or assigns, and (ii) the Court, Court personnel, and members of their immediate families.

92. The putative Class is so numerous that joinder of all members is impracticable, if not impossible. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals as evidenced by the Notice Letters that were sent out by Defendant.

93. The rights of each Class Member were violated in a virtually identical manner as a result of Defendant's willful, reckless, negligent and/or wanton actions and/or inactions.

94. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a. Whether Defendant willfully, recklessly, negligently and/or wantonly failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' PII/PHI;

b. Whether Defendant was negligent or wanton in the manner in which it stored Plaintiff's and Class Members' PII/PHI;

c. Whether Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their PII/PHI;

d. Whether Defendant breached its duty to exercise reasonable care in protecting and securing Plaintiff's and Class Members' PII/PHI;

e. Whether Defendant was negligent in failing to secure Plaintiff's and Class Members' PII/PHI;

f. Whether Defendant's failure to comply with HIPAA constitutes negligence *per se*;

g. Whether Defendant's failure to comply with Section 5 of the Federal Trade Commission Act (15 U.S.C. §45) constitutes negligence *per se*;

h. Whether Defendant breached its contracts by failing to maintain the privacy and security of Plaintiff's and Class Members' PII/PHI;

i. Whether by publicly disclosing Plaintiff's and Class Members' PII/PHI without authorization, Defendant invaded Plaintiff's and Class Members' privacy;

j. Whether by publicly disclosing Plaintiff's and Class Members' PII/PHI without authorization, Defendant breached the duty of confidence it owed to Plaintiff and Class Members;

k. Whether by publicly disclosing Plaintiff's and Class Members' PII/PHI without authorization, Defendant breached the fiduciary duties it owed to Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched when it took money from Plaintiff and Class Members and failed to provide reasonable data security measures to protect Plaintiff's and Class Members' PII/PHI;

m. Whether Plaintiff and Class Members sustained damages as a result of Defendant's failure to secure and protect their PII/PHI; and,

n. Whether injunctive relief is necessary to ensure Defendant implements reasonable security measures to protect the PII/PHI of Plaintiff and the Class Members against any future data breaches by Defendant.

95. Plaintiff's claims are typical of Class Members' claims in that Plaintiff's claims and Class Members' claims all arise from Defendant's failure to properly secure, safeguard and protect Plaintiff's and Class Members' PII/PHI and the resulting Data Breach.

96. Plaintiff and his counsel will fairly and adequately represent the interests of Class Members. Plaintiff has no interests antagonistic to, or in conflict with, Class Members' interests.

Plaintiff's lawyers are experienced class action litigators and intend to vigorously prosecute this action on behalf of Plaintiff and Class Members.

97. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and Class Members' claims. Plaintiff and Class Members have been irreparably harmed as a result of Defendant's wrongful actions and/or inactions. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's failure to secure, safeguard and protect Plaintiff's and Class Members' PII/PHI.

98. Class certification, therefore, is appropriate pursuant to F.R.C.P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

99. Class certification also is appropriate pursuant to F.R.C.P. 23(b)(2) because Defendant has acted or refused to act on grounds generally applicable to the class, thereby making final injunctive relief appropriate with respect to the putative class as a whole.

100. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/WANTONNESS

101. Plaintiff re-adopts and re-alleges the factual allegations contained in the preceding paragraphs, and further allege as follows.

102. Defendant had a duty to exercise reasonable care in obtaining, using, retaining, securing, safeguarding, and protecting Plaintiff's and Class Members' PII/PHI in its possession, including implementing federal, state, and industry standard security procedures sufficient to

reasonably protect PII/PHI from unauthorized third parties.

103. Defendant owed a duty of care to Plaintiff and Class Members because it was reasonably foreseeable that its failure to adequately safeguard the PII/PHI in accordance with federal, state, and industry standards for data security would result in the compromise of that PII/PHI and failing to safeguard the private information would be a conscious disregard and would put the Plaintiff and Class Members at an increased, imminent risk of substantial harm and identity theft.

104. Defendant negligently and/or wantonly violated its duty by failing to exercise reasonable care in securing, safeguarding, and protecting Plaintiff's and Class Members' PII/PHI (as set forth in detail above).

105. Defendant acted with conscious disregard for Plaintiff's and Class Members' PII/PHI because Defendant was aware of other data healthcare data breaches prior to this Data Breach, yet Defendant chose to do nothing to strengthen its cybersecurity to protect Plaintiff's data.

106. Defendant's conduct set forth herein was so reckless and so charged with indifference and conscious disregard to the consequences of its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class Members' PII/PHI (as set forth above) as to amount to wantonness under Alabama law.

107. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII/PHI would result in an unauthorized third-party gaining access to such information for no lawful purpose.

108. Plaintiff and the Class Members have suffered (and continue to suffer) actual, injuries-in-fact, and damages as a direct and/or proximate result of Defendant's failure to secure,

safeguard and protect their PII/PHI in the form of, inter alia, (i) improper disclosure of their PII/PHI; (ii) loss of privacy; (iii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iv) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and (vi) anxiety and emotional distress—for which they are entitled to compensation.

109. Defendant's wrongful actions and/or inaction (as described above) constituted negligence and/or wantonness at common law.

COUNT II
NEGLIGENCE *PER SE*

110. Plaintiff re-adopts and re-alleges the factual allegations contained in the preceding paragraphs, and further allege as follows.

111. Federal and state statutory law and applicable regulations, including HIPAA's Privacy Rule, Section 5 of the Federal Trade Commission Act (15 U.S.C. §45) set forth and otherwise establish duties in the industry that were applicable to Defendant and with which Defendant was obligated to comply at all relevant times hereto.

112. Defendant violated these duties by failing to secure, safeguard and protect the Plaintiff's and Class Members' PII/PHI, which resulted in an unauthorized disclosure of the Plaintiff's and the Class Members' PII/PHI.

113. The purpose of HIPAA's Privacy Rule is to define and limit the circumstances in which the protected health information of individuals such as the Plaintiff and Class Members may be used or disclosed. The stated purpose of HIPAA's Privacy Rule was also to establish minimum standards for safeguarding the privacy of patient's individually identifiable health information.

114. Defendant was also prohibited by the FTC Act from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). Various FTC publications and orders also form the basis of Defendant's duty.

115. Defendant violated Section 5 of the FTC Act by failing to maintain reasonable and appropriate data security for its Patients' PII/PHI.

116. The unauthorized disclosure of the Plaintiff's and Class Members' PII/PHI at issue in this action was exactly the type of conduct that the legislation referenced above was intended to prohibit, and the harm at issue in this case that has been suffered by the Plaintiff and Class Members is the type of harm the legislation referenced above was intended to prevent.

117. Plaintiff and Class Members, as owners of the sensitive personally identifying information that Defendant failed to protect, fall within the class of persons HIPAA's Privacy Rule and the FTC Act. were intended to protect.

118. The harm suffered and that may be suffered in the future by the Plaintiff and Class Members is the same type of harm HIPAA's Privacy Rule and the FTC Act were intended to guard against.

119. As a direct and proximate result of Defendant's violation of HIPAA's Privacy Rule and the FTC Act, Plaintiff and Class Members were damaged in the form of, without limitation, loss of time monitoring credit reports and financial accounts and placing credit freezes, expenses for credit monitoring and insurance, expenses for periodic credit reports, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

COUNT III
BREACH OF EXPRESS AND/OR IMPLIED CONTRACT

120. Plaintiff re-adopts and re-alleges the factual allegations contained in the preceding paragraphs, and further allege as follows.

121. Defendant offered to provide goods and services to Plaintiff and Class Members in exchange for payment and required Plaintiff and Class Members to provide Defendant with their PII/PHI in order to receive such goods and services.

122. Defendant had a written agreement and understanding with the Plaintiff and the Class Members as set forth in Defendant's Notice of Privacy Practices that Defendant would not disclose Plaintiff's or the Class Members' confidential information in a manner not authorized by applicable law or industry standards.

123. Defendant's Notice of Privacy Practices provided to Plaintiff and the Class Members constitutes an express contract or at the very least created a meeting of the minds that was inferred from the conduct of the parties. Plaintiff and the Class Members fully discharged their obligations under the contract.

124. Further, Alabama law imposes on physicians and health care professionals an implied contract of confidentiality that is breached by the unauthorized release of medical information, and Defendant breached those implied contracts with Plaintiff and Class Members when it released their PII/PHI to unauthorized third parties.

125. Defendant materially breached its contracts with Plaintiff and Class Members by failing to secure, safeguard and protect Plaintiff's and Class Members' PII/PHI such that an unauthorized disclosure of Plaintiff's and Class Members' PII/PHI occurred.

126. As a direct and proximate result of Defendant's breach of its contracts with Plaintiff and Class Members, Plaintiff and Class Members have been, and continue to be, damaged

in an amount to be proven at trial.

127. As further damages, Plaintiff and Class Members request restitution and costs of mitigation including, but necessarily limited to, the purchase of credit monitoring, credit insurance, periodic credit reports and expenses associated with the loss or replacement of their valuable PII/PHI included in the Data Breach.

COUNT IV
UNJUST ENRICHMENT

128. Plaintiff re-adopts and re-alleges the factual allegations contained in the preceding paragraphs, and further allege as follows.

129. Plaintiff brings this claim in the alternative to their Implied Contract claim.

130. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, Plaintiff and Class Members purchased goods and services from Defendant and provided Defendant with their private information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their private information with adequate data security.

131. Defendant knew that Plaintiff and Class Members conferred a benefit on Defendant and have accepted or retained that benefit. Defendant profited from Plaintiff's purchases and used Plaintiff's and Class Members' private information for business purposes.

132. Defendant failed to secure Plaintiff's and Class Members' private information and, therefore, did not fully compensate Plaintiff and Class Members for the value that their private information provided.

133. Defendant acquired the private information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

134. If Plaintiff and Class Members knew that Defendant would not secure their private information using adequate security, they would have made alternative healthcare choices that excluded Defendant.

135. Plaintiff and Class Members have no adequate remedy at law.

136. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on it.

137. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid.

RELIEF REQUESTED

138. Plaintiff re-adopts and re-alleges the factual allegations contained in the preceding paragraphs, and further allege as follows.

139. **DAMAGES.** As a direct and/or proximate result of Defendant's wrongful actions and/or inactions (as described above), Plaintiff and Class Members suffered (and continue to suffer) damages in the form of, *inter alia*: (i) the untimely and/or inadequate notification of the Data Breach; (ii) improper disclosure, dissemination and publication of their PII/PHI; (iii) criminal misuse of their PII/PHI; (iv) loss of privacy; (v) suspected and/or actual identity theft /financial fraud; (vi) loss of privacy; (vii) out-of-pocket expenses incurred to mitigate the identity theft and financial fraud and the continued increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (viii) economic losses relating to the theft of their PII/PHI; (ix) the value of their time spent mitigating suspected and/or actual identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (x) deprivation of the value of their PII/PHI,

for which there is a well-established national and international market; and (xi) stress, anxiety and emotional distress. Plaintiff's and Class Members' damages were foreseeable by Defendant.

140. **EXEMPLARY DAMAGES.** Plaintiff and Class Members also are entitled to exemplary damages to punish Defendant and to deter such wrongful conduct in the future.

141. **INJUNCTIVE RELIEF.** Plaintiff and Class Members also are entitled to injunctive relief in the form of, without limitation, requiring Defendant to, *inter alia*, (i) immediately disclose to Plaintiff and Class Members the precise nature and all details known to Defendant regarding the Data Breach, (ii) immediately secure the PII/PHI of its past, present, and future patients, (iii) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any future data breaches, (iv) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, (v) submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control, (vi) implement training for its personnel on new or modified security procedures through education programs, policies and tests, and (vii) pay for, not less than three years, identity theft and credit monitoring services for Plaintiff and Class Members.

WHEREFORE, Plaintiff, on behalf of himself and Class Members, respectfully request that (i) Defendant be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiff be designated the Class Representative, and (iv) Plaintiff's counsel be appointed as Class Counsel. Plaintiff, on behalf of himself and Class Members, further request that upon final trial or hearing, judgment be awarded against Defendant, in favor of Plaintiff and the Class Members, for:

i. actual damages, consequential damages, and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

ii. exemplary damages;

iii. injunctive relief as set forth above;

iv. pre- and post-judgment interest at the highest applicable legal rates;

v. costs of suit and attorneys' fees; and,

vi. such other and further relief that this Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and all others similarly situated, respectfully demands a trial by jury on all of the claims and causes of action so triable.

Dated: June 6, 2025

Respectfully submitted,

/s/ Jon Mann

Jonathan S. Mann (ASB-1083-A36M)
Austin B. Whitten (ASB-7228-K13Y)
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Email: jonm@pittmandutton.com
Email: austinw@pittmandutton.com

Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Law Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200
E: ostrow@kolawyers.com

Counsel for Plaintiff and the Proposed Class

EXHIBIT A

BRADFORD HEALTH SERVICES

Return Mail Processing Center
P.O. Box 1907
Suwanee, GA 30024

[redacted]

5 1 1654 **********AUTO**MIXED AADC 302
Paul Wiezorek
[redacted]

May 30, 2025

Subject: Notice of Data Security Incident

Dear Paul Wiezorek:

We are writing to inform you about a data security incident experienced by Bradford Health Services ("Bradford Health") that may have involved your personal and / or protected health information. Bradford Health takes the privacy and security of all information within its possession very seriously. That is why we are writing to notify you of the incident and provide you with information about steps you can take to help protect your information.

What Happened. On December 8, 2023, Bradford Health detected unusual activity within its network. Upon discovery, we immediately took steps to secure our network and engaged a leading, independent digital forensics and incident response firm to investigate. Based on that investigation, Bradford Health learned that an unknown actor gained unauthorized access to our network and acquired certain files, some of which contained individuals' personal and / or protected health information. With the assistance of a third-party data review team, we conducted a comprehensive review of all potentially impacted data to identify the individuals and information involved. On May 15, 2025, we determined that your information was impacted.

What Information Was Involved. The information that was potentially impacted during this incident may have included your name, as well as your date of birth, physician name, health care dates of service, treatment information or diagnosis treatment or procedure information, Medical Record Number (MRN), Patient Account Number (PAN), full face photograph or comparable photograph.

What Are We Doing. As soon as Bradford Health discovered the incident, we took the steps described above and implemented measures to enhance the security of our network and reduce the risk of a similar incident occurring in the future. Bradford also reported the incident to law enforcement and is cooperating with any resulting investigation.

What Can You Do. You can follow the recommendations on the following pages.

For More Information: If you have questions or need assistance, please contact 1-877-670-4122 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Andy Seitz
Chief Compliance Officer

Bradford Health Partners
2101 Magnolia Avenue South, Suite 518
Birmingham, AL 35205